UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,491	09/21/2004	Arthur Rothstein	VIV/0013.02	5490

28653 7590 10/03/2006

JOHN A. SMART
708 BLOSSOM HILL RD., #201
LOS GATOS, CA 95032

EXAMINER	
RUSSELL, TRACI L	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/711,491	**Applicant(s)** ROTHSTEIN, ARTHUR
	Examiner Traci L. Russell	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/21/2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Pursuant to U.S.C. 131, claims 1-60 have been examined.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-12, 14-28, 30-58, and 60 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

3. Claim 1 discloses a method for securing a program comprised of a plurality of interoperable components, the method comprising: extracting information about a function of a first component of the program that is callable by at least one other component of the program; securing the extracted information; in response to an attempt by a second component of the program to invoke the function of the first component, validating authenticity of the second component; and if the second component is validated, providing access to the function of the first component using the secured extracted information.

It appears that the claim is directed to a practical application; however, the limitations fail to produce a useful, concrete, and tangible result. The indicating step is conditional and the result has not been utilized nor made available in such a manner that any usefulness of having performed the validation can be realized. Appropriate amendment to the claim is required to continue the process until there is a tangible result.

4. Claims 14, 30, and 60 disclose a downloadable set of processor-executable instructions for performing the method of the claim. The claims disclose functional-descriptive material per se. The downloadable instructions fail to include the hardware necessary to realize the functionality. Appropriate amendment to the claims is required.

5. Claims 15 and 45 disclose a method for securing an exported function of a program, the method comprising: extracting export information about the exported function of the program; securing the extracted export information; intercepting an attempt to access the exported function by an importer; authenticating the importer for determining whether to permit access to the exported function; and if the importer is authenticated, providing access to the exported function based on the secured extracted export information. The 'importer' appears to be software per se, which lack necessary physical articles or objects. The claims also fail to disclose how the exported function will be secured. Appropriate amendment to the claims is required.

6. Claim 31 disclose a system for securing a program comprised of a plurality of interoperable components, the system comprising: a module for extracting information about a function of a first component of the program that is callable by at least one other component of the program; a module for securing the extracted information; a validation

module for validating authenticity of a second component attempting to invoke the function of the first component and a security module for blocking the attempt to invoke the function of the first component if the second component cannot be authenticated. Each module would reasonably be interpreted as software routines, which is a system of software per se, and lacks the necessary physical articles or objects as components to make it a machine or manufacture. Appropriate amendment to the claim is required.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless – (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-10, 12-19, 21-22, 24-37, 39-42, 45, 48-54, and 56-60 are rejected under 35 U.S.C. 102(b) as being anticipated by Ferguson (US 5,933,826).

(1) with regard to claim 1:

A method for securing a program comprised of a plurality of interoperable components, the method comprising:

extracting information about a function [step 83, Col 8, lines 33-34] of a first component of the program that is callable by at least one other component of the program ['interpreter'; Col 8, lines 35-36];

securing the extracted information [Col 8, lines 38-39]; in response to an attempt by a second component of the program to invoke the function of the first component, validating authenticity of the second component [Col 8, lines 45-48]; and

if the second component is validated, providing access to the function of the first component using the secured extracted information [Col 8, lines 49-52].

(2) with regard to claim 2:

The method of claim 1, further comprising:

generating a signature for the second component, so as to enable authentication of the second component [Col 6, lines 64-65; Col 8, lines 10-12].

(3) with regard to claim 3:

The method of claim 2, wherein said step of generating a signature includes generating a signature includes generating a selected one of an Authenticode signature and an MD5 message digest [Col 6, lines 66-67].

(4) with regard to claim 4:

The method of claim 2, wherein said step of generating a signature includes generating a hash ['value'; Col 2, lines 61-64] of the second component and encrypting the hash with a private key ['encryption system'; Col 8, lines 37-40].

(5) with regard to claim 5:

The method of claim 4, wherein said validating step includes decrypting the hash with a public key and comparing the hash to a known value [Col 8, lines 58-60].

(6) with regard to claim 6:

The method of claim 1, wherein said extracting step includes extracting information from an export table of the first component [Col 9, lines 43-45].

(7) with regard to claim 7:

The method of claim 1, wherein said extracting step includes removing the function name from an export table of the first component [' executing program'; Col 9, lines 43-50].

(8) with regard to claim 8:

The method of claim 1, wherein said securing step includes obscuring the function name ['encrypted'; Col 9, lines 58-59].

(9) with regard to claim 9:

The method of claim 1, wherein said securing step includes creating a secure export table for securing the extracted information ['target attribute'; Col 9, lines 15-20].

(10) with regard to claim 10:

The method of claim 1, wherein said providing step includes routing a call by the second component to the function of the first component ['interpreter'; Col 2, lines 6-10].

(11) with regard to claim 12:

The method of claim 1, wherein said extracting step includes extracting information about a function of the first program specified by a user [Col 9, lines 43-45].

(12) with regard to claim 13:

A computer-readable medium having processor-executable instructions for performing the method of claim 1[Fig 5, block 91; Col 9, lines 4-6].

(13) with regard to claim 14:

A downloadable set of processor-executable instructions for performing the method of claim 1 [Col 9, lines 25-27].

(14) with regard to claim 15:

A method for securing a program comprised of a plurality of modules, at least one of the modules having export information for allowing other modules to invoke its program code, the method comprising:

generating signatures for at least some of the program's modules [Col 6, lines 66-67];

as the program is loaded, validating said signatures so as to verify authenticity of respective modules of the program [Col 8, lines 45-48];

for each module having program code that may be invoked by another module, removing that module's export information [Col 8, lines 33-34];

securely storing any removed export information [Col 8, lines 38-39];

for each module having its export information removed, blocking any attempt from another module to invoke its program code if the other module cannot be authenticated [Col 8, lines 44-46]; and

if the other module is authenticated, allowing the attempt to proceed using the securely stored export information [Col 8, lines 49-52].

(15) with regard to claim 16:

The method of claim 15, wherein said generating step includes generating a selected one of an Authenticode signature and an MD5 message digest [Col 6, lines 66-67].

(16) with regard to claim 17:

The method of claim 15, wherein said generating step includes generating a hash ['value'; Col 2, lines 61-64] of a module and encrypting the hash with a private key [Col 8, lines 37-38].

(17) with regard to claim 18:

The method of claim 17, wherein said validating step includes decrypting the hash ['value'; Col 2, lines 61-64] with a public key and comparing the hash to a known value [Col 8, lines 58-60].

(18) with regard to claim 19:

The method of claim 15, further comprising:

providing a security module for validating authenticity of a module ['access control mechanism'; Col 8, lines 26-29].

(19) with regard to claim 21:

The method of claim 19, wherein an attempt to invoke a module having its export information removed is routed to the security module ['encryption system'; Col 8, lines 38-41].

(20) with regard to claim 22:

The method of claim 21, wherein the security module allows the attempt to proceed if the other module making the attempt is authenticated ['suitable access rights'; Col 8, lines 49-52].

(21) with regard to claim 24:

The method of claim 15, wherein said removing step includes removing export information for a particular module specified by a user ['step 88', Col 8, lines 57-62].

(22) with regard to claim 25:

The method of claim 15, wherein said removing step includes removing information from an export table [Col 9, lines 43-45].

(23) with regard to claim 26:

The method of claim 15, wherein said securely storing step includes obscuring removed export information ['encryption'; Col 9, lines 58-59].

(24) with regard to claim 27:

The method of claim 15, further comprising:

in response to an attempt to invoke program code of a given module, verifying authenticity of the given module and blocking the attempt if the given module cannot be authenticated ['access control mechanism'; Col 8, lines 45-48].

(25) with regard to claim 28:

The method of claim 15, further comprising:

after allowing the attempt to proceed, providing for subsequent attempts by the other module to invoke the program code to directly invoke the program code ['suitable access rights'; Col 8, lines 49-52].

(26) with regard to claim 29:

A computer-readable medium having processor-executable instructions for performing the method of claim 15 [Col 9, lines 4-6].

(27) with regard to claim 30:

A downloadable set of processor-executable instructions for performing the method of claim 15 [Col 9, lines 25-27].

(28) with regard to claim 31:

A system for securing a program comprised of a plurality of interoperable components, the system comprising:

a module for extracting information about a function of a first component [Col 8, lines 33-34] of the program that is callable by at least one other component of the program [Col 8, lines 35-36];

a module for securing the extracted information [Col 8, lines 38-39];

a validation module for validating authenticity of a second component attempting to invoke the function of the first component [Col 8, lines 45-48]; and

a security module for blocking the attempt to invoke the function of the first component if the second component cannot be authenticated ['access control mechanism'; Col 8, lines 45-48].

(29) with regard to claim 32:

The system of claim 31, wherein the validation module validates authenticity of the second component based on examining a digital signature of the second component [Col 7, lines 2-4].

(30) with regard to claim 33:

The system of claim 31, further comprising:

a module for generating a signature for at least some components of the program, so as to enable authentication of said at least some modules [Col 6, lines 64-65; Col 8, lines 10-12].

(31) with regard to claim 34:

The system of claim 33, wherein the module for generating generates a selected one of an Authenticode signature and an MD5 message digest [Col 6, lines 66-67].

(32) with regard to claim 35:

The system of claim 33, wherein the module for generating generates a hash of a module and encrypts the hash with a private key [Col 8, lines 37-38].

(33) with regard to claim 36:

The system of claim 35, wherein the validation module decrypts the hash with a public key and compares the hash to a known value [Col 8, lines 58-60].

(34) with regard to claim 37:

The system of claim 31, wherein the security module routes the attempt to the function of the first module if the second module is authenticated [Col 8, lines 37-48; Col 10, lines 2-4].

(35) with regard to claim 39:

The system of claim 31, wherein the module for extracting removes an export table entry for the function of the first module [Col 9, lines 43-45].

(36) with regard to claim 40:

The system of claim 31, wherein the module for securing creates a secure export table including the extracted information [Col 9, lines 15-20].

(37) with regard to claim 41:

The system of claim 40, wherein the secure export table is created without using a clear text name for the function of the first module [Fig 3; Col 8, lines 12-13].

(38) with regard to claim 42:

The system of claim 40, wherein the module for securing obscures function names in the secure export table [Fig 3; Col 9, lines 58-60].

(39) with regard to claim 45:

A method for securing an exported function of a program, the method comprising: extracting export information about the exported function of the program [Col 8, lines 34-36];

securing the extracted export information [Col 8, lines 38-39];

intercepting an attempt to access the exported function by an importer [Col 8, lines 45-47];

authenticating the importer for determining whether to permit access to the exported function [Col 8, lines 49-52]; and

if the importer is authenticated, providing access to the exported function based on the secured extracted export information [Col 8, lines 60-62].

(40) with regard to claim 48:

The method of claim 45, further comprising:

if the importer cannot be authenticated, blocking access to the exported function [Col 9, lines 66-67; Col 10, line 1].

(41) with regard to claim 49:

The method of claim 45, wherein said authenticating step includes authenticating the importer based on a digital signature of the importer [Col 7, lines 2-4].

(42) with regard to claim 50:

The method of claim 45, further comprising:

generating a digital signature for at least some executable modules of the program, so as to enable authentication of said at least some executable modules [Col 6, lines 64-65; Col 8, lines 10-12].

(43) with regard to claim 51:

The method of claim 50, wherein said generating step includes generating a selected one of an Authenticode signature and an MD5 message digest [Col 6, lines 66-67].

(44) with regard to claim 52:

The method of claim 50, wherein said authenticating step includes validating digital signature of the importer [Col 7, lines 2-3].

(45) with regard to claim 53:

The method of claim 45, further comprising: authenticating a program module including the exported function before providing access to the exported function [Col 7, lines 4-6].

(46) with regard to claim 54:

The method of claim 45, wherein said providing step includes routing a call by the importer to the exported function ['interpreter', Col 2, lines 6-10].

(47) with regard to claim 56:

The method of claim 45, wherein said extracting step includes removing an export table entry for the exported function [Col 9, lines 43-45].

(48) with regard to claim 57:

The method of claim 45 wherein said securing step includes obscuring the exported function name [Col 9, lines 58-59].

(49) with regard to claim 58:

The method of claim 45, wherein said securing step includes creating a secure export table based on the extracted export information ['target attribute'; Col 9, lines 15-20].

(50) with regard to claim 59:

A computer-readable medium having processor-executable instructions for performing the method of claim 45 [Col 9, lines 4-6].

(51) with regard to claim 60:

A downloadable set of processor-executable instructions for performing the method of claim [Col 9, lines 25-27].

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 11, 20, 23, 38, 43-44, 46-47, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ferguson, in view of Idoni (US 2004/0123308).

with regard to claims 11, 23, 38, and 55:

Ferguson teaches a method for securing a program comprised of a plurality of interoperable components, comprising: extracting information about a function [Col 8, lines 33-34] of a first component of the program that is callable by at least one other component of the program [Col 8, lines 35-36]; a method of transparent data delivery comprising: securing the extracted information [Col 8, lines 38-39]; in response to an attempt by a second component of the program to invoke the function of the first component, validating authenticity of the second component [Col 8, lines 45-48]; and if the second component is validated, providing access to the function of the first component using the secured extracted information [Col 8, lines 49-52].

Ferguson does not teach returning an address of the function as required in claims 11, 23, 38, and 55.

However, Idoni teaches a method that provides a step that includes returning a address of the function if authenticated [Col 3, paragraph 0031]. The 'physical location' disclosed by Idoni is interpreted by the Examiner as the return address of the function or module. Furthermore, the method taught by Idoni provides the advantage of both implicit and explicit linking while eliminating much of the programmatic and associated overhead at design, implementation and execution time [Col 2, paragraph 0017].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to recognize that the identification and physical location of a function used in the method taught by Idoni would have been implemented in the method disclosed by Ferguson in order to identify the physical location of the dynamic link loader [Col 3, lines 16-19]. Access can then be regulated to preserve security.

5. with regard to claim 20:

Ferguson teaches all the subject matter above with the exception of the security module includes instructions causing the security module to be initialized before other modules of the programs as required in claim 20.

However, the method disclosed by Idoni teaches instructions causing a module to be initialized before other modules ['dynamic linking'; Col 1, paragraph 0008] and teaches that implicit linkage has the advantage that execution is rapid since the DLL is pre-loaded into memory and statically linked references are resolved by the system when a program is loaded [Col 1, paragraph 0010].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of dynamic linking as disclosed by Idoni in the access control mechanism to control access to the distributed directory disclosed by Ferguson because implicit linkage has the advantage of rapid execution since the dynamic link loader is pre-loaded into memory and statically linked references are resolved by the system when a program is loaded [Col 1, paragraph 0010] thereby initializing the security module before any other modules or programs.

6. with regard to claims 43 and 44:

Ferguson teaches a system wherein the security module modifies the executable code included in the second module if the second module is authenticated so as to enable the second module to directly invoke the function of the first module [Col 8, lines 56-65] as required in claim 44.

Ferguson does not teach a system wherein the security module inserts executable code into the second module during initialization of the second module so as to direct an attempt by the second module to invoke the function of the first module to the security module as required by claim 43.

However, Idoni teaches a method that includes an identification and physical location within the loader routine [Fig 5'; Col 3, paragraph 0031]. Idoni also teaches that during program execution, when the dynamic link loader is required, the application program has already resolved the identification and reference points. Explicit linking provides greater flexibility by allowing the application program to specify entities to utilize during execution [Col 1, paragraph 0012]. In dynamic linking, prior to or during execution entities are linked together with the application program using a linker or loaded and invoked explicitly by an application. Access can then be regulated to preserve security.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of dynamic linking as taught by Idoni in the method taught by Ferguson in order to specify entities to utilize during execution, and to provide the advantage of both explicit and implicit linking [Col 2, paragraph 0017].

7. with regard to claims 46 and 47:

Ferguson teaches a method for securing an exported function of a program as required in claim 45. However, Ferguson does not teach a method wherein the importer comprises another module or another program as required in claims 46 and 47.

Idoni teaches a method that includes instructions causing a module to be initialized before other modules ['dynamic linking'; Col 1, paragraph 0008]; a method wherein the importer comprises another module [Fig 1b, Col 1, paragraph 0011] as required by claim 46.

Idoni further teaches a method wherein the importer comprises another program [Fig 1b; Col 1, paragraph 0011] as required by claim 47.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made for Ferguson to invoke the load and link method taught by Idoni in order to import and link a program by the computer system or by the program as disclosed by Idoni ['dynamic linking', Col 1, paragraph 0008] for the purpose of securing an exported function of a program to provide the advantage of both implicit and explicit linking [Col 2, paragraph 0017].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Traci L. Russell whose telephone number is 571.272.1095. The examiner can normally be reached on Mon - Fri (alternate Fridays off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 570.272.4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TLR
20060908

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/28/06